ROBUST DATA HIDING AND SECURE KEY GENERATION IN H.264 COMPRESSED VIDEOS

SRUTHI M S[1], JOBIN JOSE[2]

[1] *M. Tech student (Applied electronics and instrumentation), Dept of ECE, Lourdes Matha College of Science &Technology, Trivandrum, kerala, India*

[2] *Assistant Professor, Dept of ECE, Lourdes Matha College of Science &Technology, Trivandrum, kerala, India*

Abstract - *For providing privacy and security digital video want to be processed and stored in encrypted domain. It is necessary to perform data hiding in these encrypted videos for the purpose of content notation and/or tampering detection. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. The process involves video encryption, data embedding, and data extraction. By analyzing the property of H.264, the DCT coefficients and the motion vector differences are encrypted with stream ciphers. LFSR based stream cipher produce pseudo random strings which improve security of video transmission. Selective data hiding is utilized in the method to determine frames with less number of motion vectors which are suitable for data hiding. Furthermore this Paper introduce the system with more secure and better quality videos even after decryption. This proposed method is tested by using two parameters such as structural similarity (SSIM) and Peak signal to noise ratio (PSNR) value.*

Key Words: H.264/AVC, Motion Vectors, Encryption, LFSR, Selective data hiding

1. INTRODUCTION

Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data has also increased. Various good techniques are proposed and already taken into practice. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. The requirements of any data hiding system can be categorized into security, capacity and robustness. The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help address the security and privacy concerns with cloud computing. For example, a cloud server can embed the additional information (e.g., video notation, or authentication data) into an encrypted version of an H.264/AVC video by using data hiding technique. With the hidden information, the server can manage the video or verify its integrity without knowing the original content, and thus the security and privacy can be protected. This technology can be applied to prominent scenarios. For example, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain.

The purpose of hiding such information depends on the application and the needs of the owner/user of the digital media. Data hiding requirements include the following:

a. Imperceptibility- The video with data and original data source should be
perceptually identical.
b. Robustness- The embedded data should survive any processing operation the host
signal goes through and preserve its fidelity.
c. Capacity-Maximize data embedding payload.
d. Security- Security is in the key.

The process involves three parts: encryption, data hiding and data extraction. Data encryption is a suitable method to protect data. Both DCT coefficients and motion information (MVD) are encrypted during H.264/AVC encoding. Data can be embedded in encrypted domain. There are several methods for data hiding in video frames. One of the method, embed secret data directly in compressed and then encrypted H.264/AVC bit stream. With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the near future. Obviously, due to the constraint of the underlying encryption, it is very difficult and sometimes impossible to transplant the existing data hiding algorithms to the encrypted domain.

2. RELATED WORK

W. J. Lu, A. Varna, and M. Wu [1], The application scenario of providing functionality over encrypted private videos stored online. We studied three representative processing tasks, namely, video search, classification, and summarization, and discussed related techniques and remaining challenges. Given the large size and rich information of video data, it is important to design highly efficient yet privacy-aware processing techniques. The

future advancement in cryptography can open up possibilities for a complete range of secure processing and editing operations for private videos stored online.

B. Zhao, W. D. Kou, and H. Li [2], An enhanced watermarking scheme is proposed to improve in terms of increasing effective watermarking capacity, avoiding additional overhead and overcoming an inherent flaw that watermarking capacity depends on the probability distribution of input watermark sequence. Based on the enhanced scheme, a new watermarking scheme in the encrypted domain is proposed with flexible watermarking capacity. Encrypted Data Hiding in Video Stream using Code Word Substitution (IJSTE/ Volume 1 / Issue 9 / 008) All rights reserved by www.ijste.org

P. J. Zheng and J. W. Huang [3], Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which reserving room before encryption is proposed. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

X. P. Zhang [4], A RDH method for encrypted images by shifting the encrypted histogram of predicted errors, and achieves excellent performance in three aspects: complete reversibility, higher PSNR under given embedding rate, separability between data extraction and image decryption. Our method can work on two schemes independently in order to suit different application prospects by extracting the data from the encrypted image or from the decrypted image.

Z. Shahid, M. Chaumont, and W. Puech [5], Encryption and data embedding would lead to increasing the bit-rate of H.264/AVC bitstream. On the contrary, our proposed scheme can encrypt H.264/AVC video stream directly and then embeds data into encrypted H.264/AVC video stream to meet the privacy-preserving requirements. The bit-rate of the encrypted H.264/AVC video stream containing hidden data is exactly the same as the original H.264/AVC video stream.

3. SYSTEM ARCHITECTURE

A novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which is made up of three subsequent parts, i.e., H.264/AVC video encryption, data embedding and data extraction. It is necessary to perform data hiding in the encrypted videos for the purpose of the content notation and/or tampering detection. Data hiding in encrypted Domain without decryption preserves the confidentiality of the content. By analyzing the property of H.264/AVC , the DCT coefficients and motion vector differences are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using selective data embedding method.

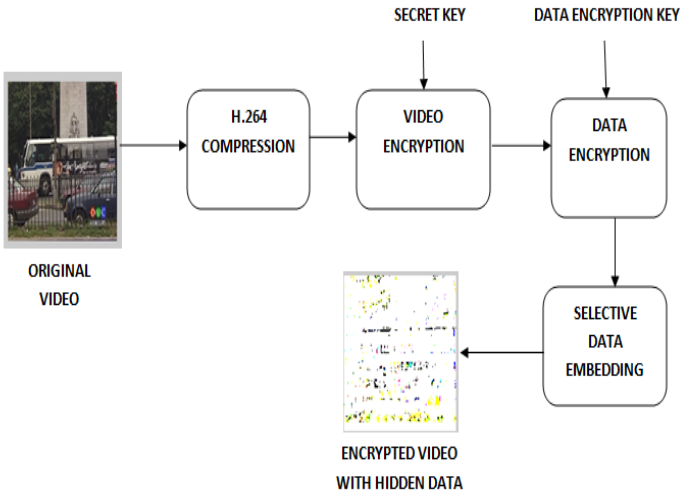


Fig -1: Video encryption and data embedding at the sender end.

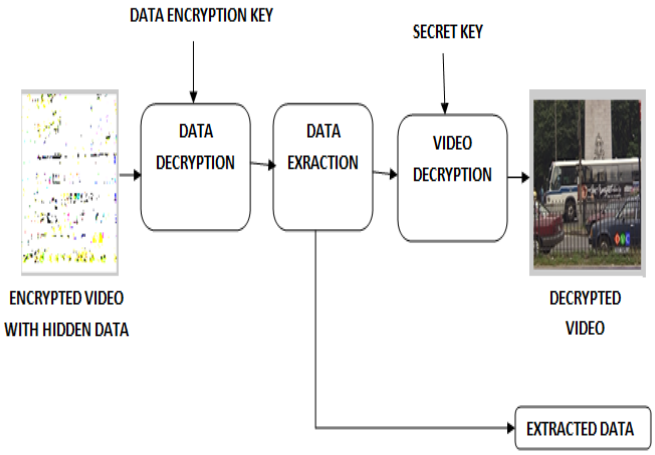


Fig -2: Data extraction and video display at the receiver end

3.1 Encryption of H.264/AVC Video Bit Stream

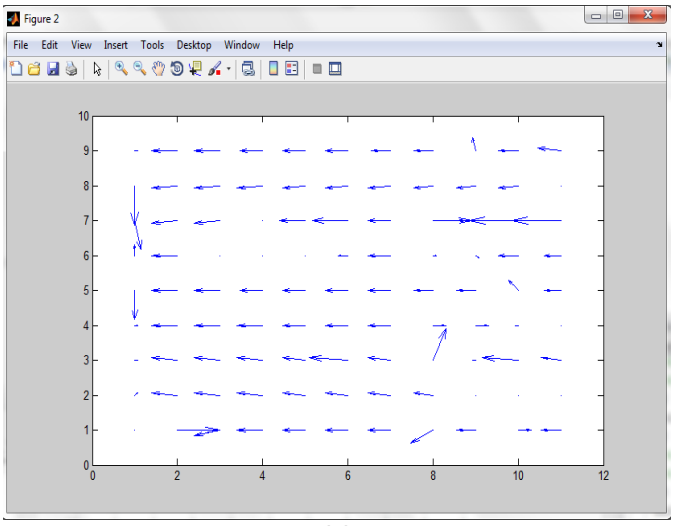
An H.264/AVC video encryption scheme with good performance including security, efficiency, and format compliance is been proposed. By analyzing the property of H.264/AVC , DCT coefficients and MVDs are encrypted with stream ciphers. For secure transmission key should be

1) *LFSR*:A linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. Thus, an LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined

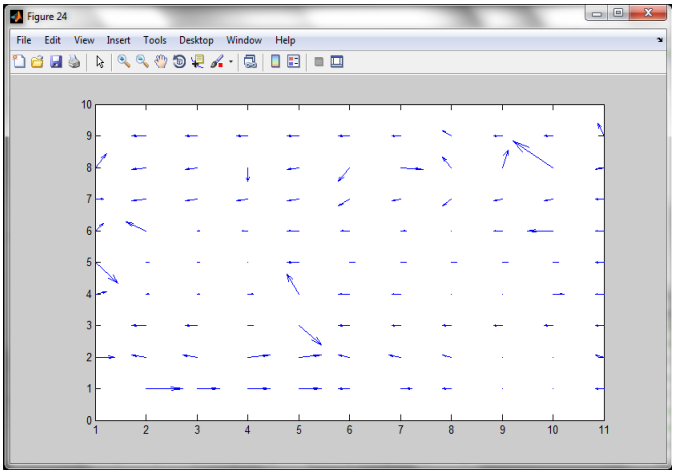
by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

2) DCT Coefficients Encryption: The transform coding developed more than two decades ago, has proven to be a very effective video coding technique, especially in spatial domain. Today, it forms the basis of almost all video coding standards. The most common transform based intra-frame video coders use the DCT (Discrete Cosine Transform) which is very close to MPEG. The main goal of the transform is to de-correlate the pixels of the input block. This is achieved by redistributing the energy of the pixels and concentrating most of it in a small set of transform coefficients. This is known as Energy compaction The DCT, which will be used in our video compression approach, is widely used in most modern image/video compression algorithms in the spatial domain (MJPEG, MPEG). DCT coefficients values are encrypted the pseudo random keys generated by LFSR.

3) Motion Vector Difference (MVD) Encryption: Further to protect both texture information and motion information, not only the DCT coefficients but also the motion vectors should be encrypted. In H.264/AVC, motion vector prediction is further carried out on the motion vectors, which yields MVD. Difference between two successive frames are encrypted with the pseudo random key.



(a)



(b)

Fig -3(a),(b): Motion Vectors of successive frames

3.2Data encryption and Selective Data Embedding

Before embedding the video into the video frames the data want to be encrypted with the secret key for providing security. Data embedding can be done on the motion vectors of the frame by selective embedding.
Step 1: Initially data converted into binary format.
Step 2: Motion vector values are extracted.
Step 3: Convert motion vector value into binary format.
Step 4: Each 2 bits from the data are embedded into the LSB of motion vector value.

For example to embed a data "Hello" into the motion vector values ,the data and MVD values converted into binary values. "01101000 01100101 01101100 01101100 01101111" are the binary values of text "HELLO". For embedding these values 20 MVD values are required. First two bits are embedded into the first motion vector value and so on. Embedding of values done on the smoothening region to reduce the degradation. Hence called selective embedding.

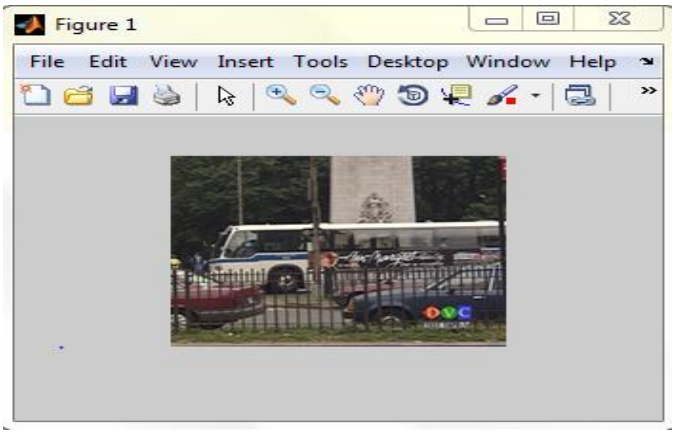


Fig -4 Original Video

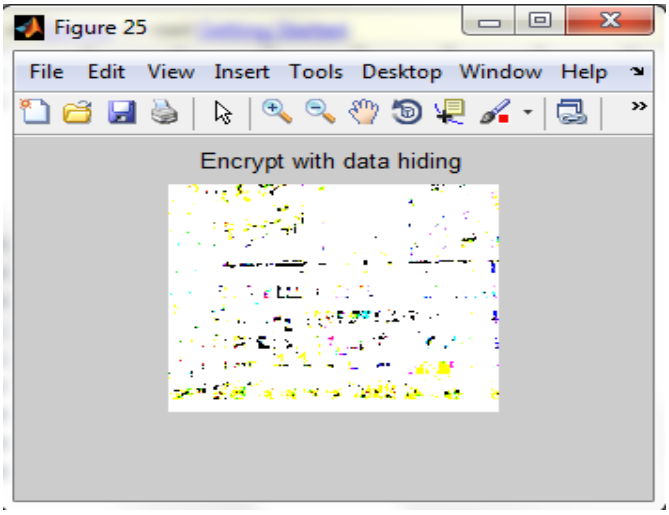


Fig -5: Encrypted video with hidden data

3.3 Data Decryption and Extraction

Data can be extracted from the motion vectors. To get the original data the extracted data want to be decrypted with the same secret key used for encryption process. Pseudo random keys are used for the the encryption and decryption process.

4. EXPERIMENTAL RESULTS

The proposed data hiding scheme has been implemented in the H.264/AVC reference software version MATlab 2010 four well-known standard video sequences (i.e., News, Football, Bus, and Space) in y4m format (176×144) at the frame rate 30 frames/s are used for simulation. The first 100 frames in each video sequence are used in the experiments. The GOP (Group of Pictures) structure is "IPPPP: one I frame followed four P frames".

A. Security of Encryption Algorithm

For the proposed video encryption scheme, the security includes both cryptographic security and perceptual security. Cryptographic security denotes the security against cryptographic attacks, which depends on the ciphers adopted by the scheme. In the proposed scheme, the secure stream cipher is used to encrypt the bitstream, and pseudo-random sequence generated by LFSR is used to encrypt the additional data. They have been proved to be secure against cryptographic attacks. Perceptual security refers to whether the encrypted video is unintelligible or not. Generally, it depends on the encryption scheme's properties. For example, encrypting only IPM cannot keep secure enough, since the encrypted video is intelligible [6]. The proposed scheme encrypts IPM and MVD which keeps perceptual security of the encrypted video.

B. Visual Quality of Video

The encrypted video containing hidden data provided by the server should be decrypted by the authorized user. Therefore, the visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video. By modifying the compressed bitstream to embed additional data, the most important challenge is to maintain perceptual transparency, which refers to the modification of bitstream should not degrade the perceived content quality.

Besides subjective observation, PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index) have been adopted to evaluate the perceptual quality [7]. PSNR is widely used objective video quality metric. However, it does not perfectly correlate with a perceived visual quality due to nonlinear behavior of human visual system. The SSIM index lies in the range between 0 and 1, where 1 indicates the reference image is identical than the target image. Since H.264/AVC is lossy compression, in order to better illustrate the data hiding on the video quality, the visual quality of video stream should be tested. The video sequence obtained by decompressing video stream is used as the target sequence, while the original uncompressed video sequence is used as the reference video sequence. Similarly, in order to test the visual quality of video stream, the video sequence obtained by encrypting, data hiding, decrypting, and decompressing process is used as the target sequence. That is, in this case, the target video contains hidden data.

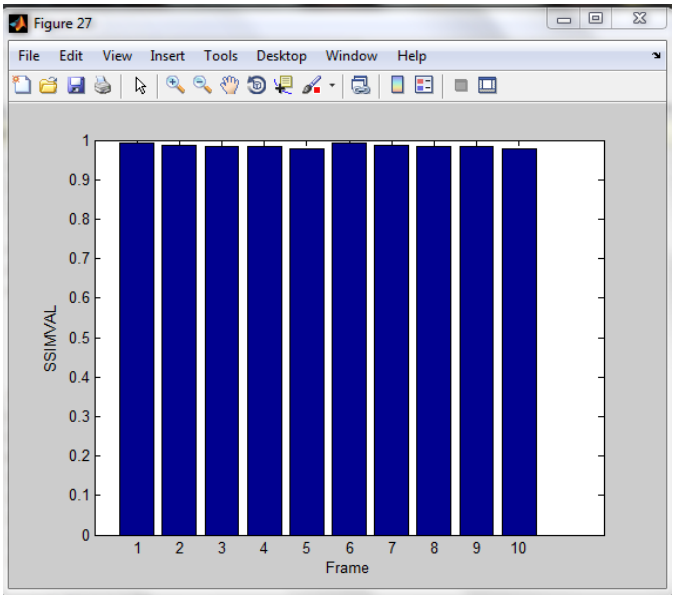


Fig -6: SSIM value representation for ten frames

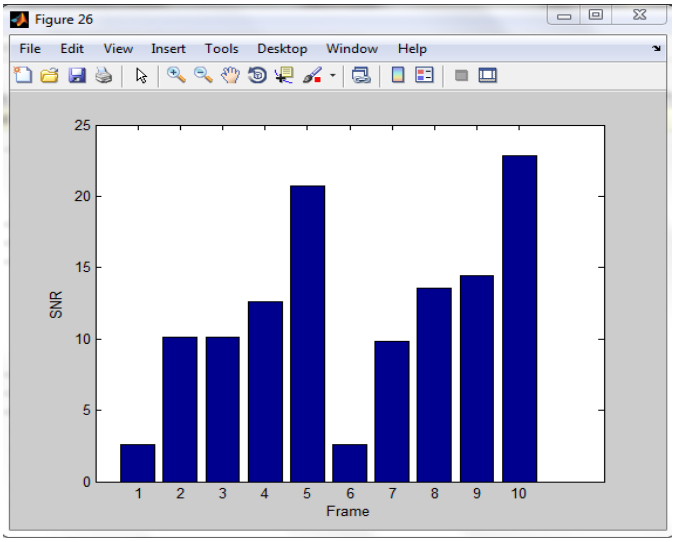


Fig -7: PSNR value representation for ten frames

5.CONCLUSION

Data activity in encrypted media could be a new topic that has started to draw attention attributable to the privacy-preserving requirements from cloud knowledge management. During this paper, an algorithm to embed extra knowledge in encrypted H.264/AVC bit stream is conferred, that consists of encryption, data embedding and extraction phases. Data embedding is straightforward to implement because it is directly performed within the compressed and encrypted domain. The hider will embed and extra data into the encrypted domain. Data hide in the slow motion. Hence the video will not be degraded .Experimental results have shown that the planned encryption and knowledge embedding theme will preserve file-size, whereas the degradation in video quality caused by knowledge activity is quite little.

ACKNOWLEDGEMENT

The author thankfully acknowledges Mr.Jobin Jose, Assistant Professor, LMCST, without whose guidance and supervision, this work would not have been possible. I would like to express my sincere gratitude to Director Prof.P.M Hormese in providing me with necessary requirements to help us to finish the work in time. I would also like to extend my whole hearted gratitude to the Head of the Department of Electronics and Communication Mr. Ram Prasad Tripathy and the PG coordinator Mrs.M.S Manju . who were always ready to help me with ideas and suggestions for rectifying the mistakes that crept up time to time during the completion of this venture. I would also like to thank my friends and last but not the least the staff of ECE department for their whole hearted support and encouragement. Above all, I am thankful to the GOD ALMIGHTY!!

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] .B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.

[3] P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking," in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.

[4] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.

[5] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[7] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," J. Real-Time Image Process., vol. 7, no. 4, pp. 205–214, 2012

